THE EMBODIMENTS OF THE INVENTION IN WHICH AN EXCLUSIVE PROPERTY OR PRIVILEGE IS CLAIMED ARE DEFINED AS FOLLOWS:

1. A method of verifying a digital signature generated by a signor in a data communication system, said signature having signature components incorporating a pair of private keys, said method comprising the steps of applying a first of said private keys to said signature to recover a value equivalent to a function associated with a second of said private keys and comparing said recovered value with said function to determine the authenticity of said signature.

2. A method according to claim 1 wherein said recovered value is used to compute a value of one of said signature components and said computed value and said signature component are compared to verify said signature.

3. A method according to claim 1 wherein the structure of said recovered value is compared with predetermined parameters to verify said signature.

4. A method according to claim 1 wherein one of said keys is a long term key and the other of said keys is a short term key generated for each signature.

5. A method according to claim 4 wherein said recovered value corresponds to said short term key.

6. A method according to claim 5 wherein said recovered value is used to compute a short term public key derived from said private key and included in said signature components.

7. A method according to claim 5 wherein at least a portion of said recovered value is hashed by a cryptographic hash function and a resultant hash value is compared to one of said signature components for verification.

8. A method of verifying a digital signature generated by a signor in a computer system, said signor having a private key d and a public key y, derived from an element g and said private key d said method comprising the steps of signing a message *m* in said computer system by:

a) generating a first signature component by combining at least said element *g* and a signature parameter *k* according to a first mathematical function;

b) generating a second signature component by mathematically combining said first signature component with said private key d, said message m and said signature parameter k; and

said signor verifying said signature by:

c) recovering a value k' from said signature without using said public key y, and ;

d) utilizing said recovered value k' in said first mathematical function to derive a value r' to verify said signature parameter k and k' are equivalent.

9. A method as defined in claim 8, wherein g is an element of order q in a field F_p^*.

10. A method as defined in claim 8, wherein g is a point of prime order n in $E(F_q)$, such that E is an elliptic curve defined over the field F_q.

11. A method as defined in claim 8, wherein said element g is a point on an elliptic curve over a finite field F_{q^r}.

12. A method as defined in claim 8, said signature parameter k being a randomly selected integer in the interval [1, q-1], and said first signature component having a form defined by $r=g^k \bmod p \bmod q$, wherein p and q are primes such that q divides $p-1$.

13. A method as defined in claim 12, including calculating a value $e = h(m)$ wherein h is a hash function, and wherein said second signature component $s = k^{-1}(e + dr) \bmod q$.

14. A method as defined in claim 13, said step of recovering said value k' including:

(a) calculating a value $z = (h(m) + dr) \bmod q$;

(b) calculating z^{-1} inverting $z \bmod q$;

(c) calculating $k'^{-1} = s(z^{-1}) \bmod q$; and

(d) calculating k' by inverting $k^{-1} \bmod q$.

15. A method as defined in claim 14, said step of verifying k including the steps of calculating $r' = g^{k'} \bmod p \bmod q$ and comparing r' to r in order to verify $k = k'$.

16. A method as defined in claim 15, including utilizing precomputed tables in said calculations.

17. A method as defined in claim 10, said signature parameter k being a statistically unique and unpredictable integer k selected in an interval [2, n-2] and said first signature component having a form defined by $r = x$, mod n wherein n is an n co-ordinate of a private key.

18. A method as defined in claim 17, including calculating a value $e = h(m)$ wherein h is a hash function and said second signature component is given by $s = k^{-1}(e + dr)$ mod n.

19. A method as defined in claim 18, said recovering said value k' includes:

(a) calculating a value $z = (h(m) + dr) \bmod n$;

(b) calculating z^{-1} by inverting z mod n;

(c) calculating $k'^{-1} = s(z^{-1}) \bmod n$, and

(d) calculating k' by inverting k^{-1} mod n.

20. A method as defined in claim 19, said step of verifying k including the steps of calculating $r' = g^{k'} \bmod n$ and comparing r' to r in order to verify $k = k'$.

21. A method as defined in claim 9, said signature parameter k being a randomly selected integer in an interval [1, p-1], and said first signature component having a form defined by $e = h(m||r)$ wherein $r = g^k \bmod p$, h is a hash function and || denotes concantenation.

22. A method as defined in claim 21, said second signature component being defined by $s = (de + k) \bmod p$.

23. A method as defined in claim 22, said step of recovering said value k' includes:

(a) calculating a value $k' = (s-de) \bmod p$;

(b) calculating a value $r' = g^k \bmod p$;

(c) calculating a value $e' = h(m||r')$; and

(d) comparing said value e' to e in order to verify $k' = k$.

24. A method of verifying the authenticity of a certificate issued by a certifying authority in an electronic data communication system, said method including the steps of said certifying authority including in said certificate a pair of signature components derived from a pair of private keys, said certifying authority retaining one of said private keys, said certifying authority receiving said certificate and applying said private key to said signature components to derive therefrom a value corresponding to a function of the other of said

private keys and comparing said derived value with said function to determine the authenticity of said certificate.

25. A method according to claim 24 wherein said derived value is compared with predetermined parameters to determine the authenticity of said certificate.

26. A method according to claim 24 wherein said derived value corresponds to said other key.

27. A method according to claim 26 wherein said one key is a long term private key used in a plurality of signatures and said other key is a short term key derived for each signature.

28. A method according to claim 26 wherein said signature components include a public key derived from said other key and said method includes the step of deriving a corresponding public key from said derived value and comparing said public key in said signature components with said corresponding public key.

29. A data communication system having a pair of correspondents connected by a data communication link, each of said correspondents having a cryptographic function to implement a public key cryptographic scheme utilising a pair of private keys, one of said private keys being utilised for multiple communications between said correspondents and the other of said private keys being generated by one of said correspondents at each communication, said one private key being shared by said correspondents to permit the other of said private keys to be recovered by said other correspondent from a digital signature generated by said one correspondent and compared to a signature component of said digital to verify the authenticity of said one correspondent.

30. A data communication system according to claim 29 wherein said cryptographic functions implement an elliptic curve cryptosystem.